A Comparative Study of Cryptographic Algorithms

Jitendra Singh Chauhan - Research Scholar, Pacific University, Pacific Hills Udaipur (Rajasthan), India

S. K. Sharma - Research Guide, Pacific University, Pacific Hills Udaipur (Rajasthan), India

Abstract: In the present Scenario, Secure data communication over network is essential and Cryptography is the best way in current scenario to ensure secure data transmission over networks. There are lots of cryptographic algorithms available and the algorithm selected for encryption and decryption must meet the basic principles of network security. The research paper focuses on the comparative study of various cryptographic algorithms like AES, DES, RSA, Blow Fish, Elliptic Curve, SHA and MD5 and give a proper direction to the users for use of proper algorithm for securing of data.

Key Words: AES, DES, RSA, Blow Fish, SHA, Elliptic Curve, MD5.

Introduction:

In the current scenario there is a past few decades there has been an uprising in technology, and leads to a maximum utilization of information technology aspects [1]. With the rapid increment of the power and use of new IT paradigm decreases the communication cost [1] [2]. IT innovation and incubation have extensive aspects across various domains of society, etc.

Cryptographic algorithms are efficient ways of securing data from cyber-attacks like indulging the contents or modification, etc. Cryptography is the practice and study of techniques for secure communication. This technique helps in protecting reliability or confidentiality of messages by converting into cipher text [1] [2].The reverse process is followed with the help of secret key. Cryptographic methods use mathematical equations for these conversions [1].

Cryptography method keeps secrecy of information by using mathematical equations and methods [3]. For the secure communication of data over network, we have to select specific type of algorithms which are more robust and perceptual to both active and passive attacks as well as from some specific attacks like noise, spatial and temporal shifts, etc. Our research focus on relative analysis of various cryptographic algorithms for specific attacks on a test set of data and find out the best suitable algorithm.

Measures of Information system security:

A reliable information communication system is said to be secure whereas information security concerns with the secure transfer of information to the authenticated and authorized users only. In the current scenario of digitization the transfer of all kind of information either it is for business purpose or fund transfer or job seeking applications, etc. follows a basic path of communication over internet which leads us to focus on the various principles of security [7].

Data communication over network is a crucial issue of information security and it needs to follow the following basic principles of security:

Confidentiality - If only the intended sender and recipient access the information, then said as data send between the sender and recipient follows the principle of confidentiality. Interception in between data communication from source and destination will cause loss of confidentiality [3] [4].

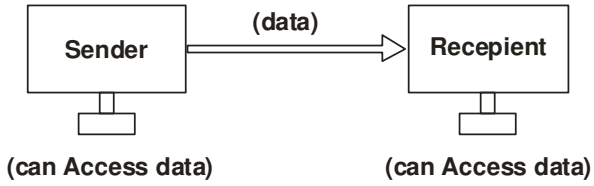

Figure:- 1.1 Confidentiality

Authentication - This is also called as proof identification or Fabrication and it is used to verify that the message is passed from the authentic user or not [4] [5].

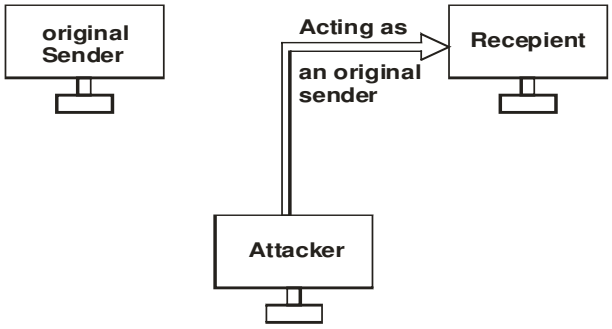

Figure:- 1.2 Fabrication Process

Integrity - If the contents of the original message is changed (modified) by the attacker for its fruitfulness (in between path of communication), then called as loss of integrity [4] [7].

Non Repudiation - If sender denies as the originator of a message, then this problem leads to loss of principle of non – repudiation. Digital signatures are the most popular way to prevent this problem and helps in maintaining the principle of non-repudiation [4] [5] [7].

Authorization – This basic principle of data security ensures the end user having permissions to perform changes or not. Authorization verifies what you are authorized to do [4] [5].

Digital Signatures:

The digital signature increases the security of an electronic message by attaching a secret code with the message which is used to judge the authenticity of the message.

These signatures generation algorithms ensures and maintains the integrity of message as shown in figure 1.3[4] [7].

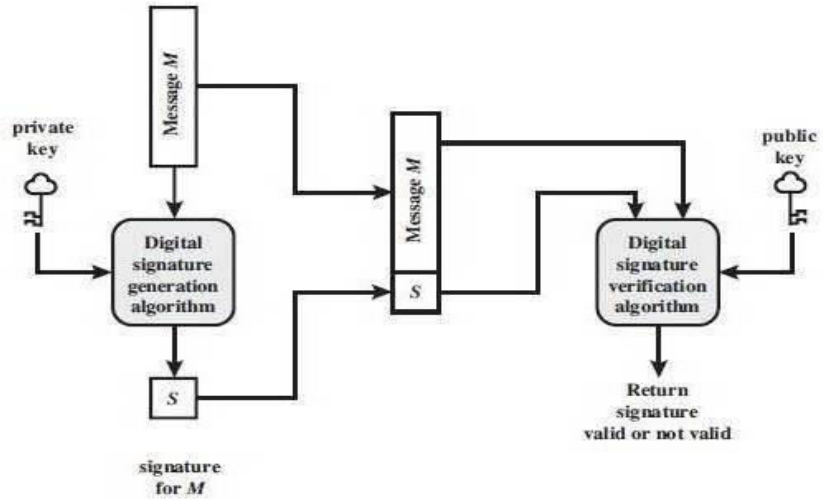

Figure 1.3 Digital Signatures

Authentication is ensured in digital signatures using certain encryption mechanism where, encryption is the process of converting the data (may be plain text, audio, images, video, etc.) into unreadable form and vice versa using some set of rules [6].

General Cryptographic Algorithms:

Data Encryption Standard (DES) – Most widely used cryptographic method for encryption. It is a more secure encryption method than others because there are 72 quadrillion or more possible encryption keys are available for use and randomly a key is chosen among this enormous number of keys but having a major problem of key distribution between sender and receiver. It follows the key expansion, compression, S – box substitution and P – box permutation and certain rotations which make it an secure standard for commercial data [4] [8] [9].

International Data Encryption Algorithm (IDEA) – It performs operation using a block of 64 -bit of plain text and a key of length 128-bit. It consist of total of eight transformations (a round, see figure 1.5). Decryption process is similar to encryption process. [4] [8].

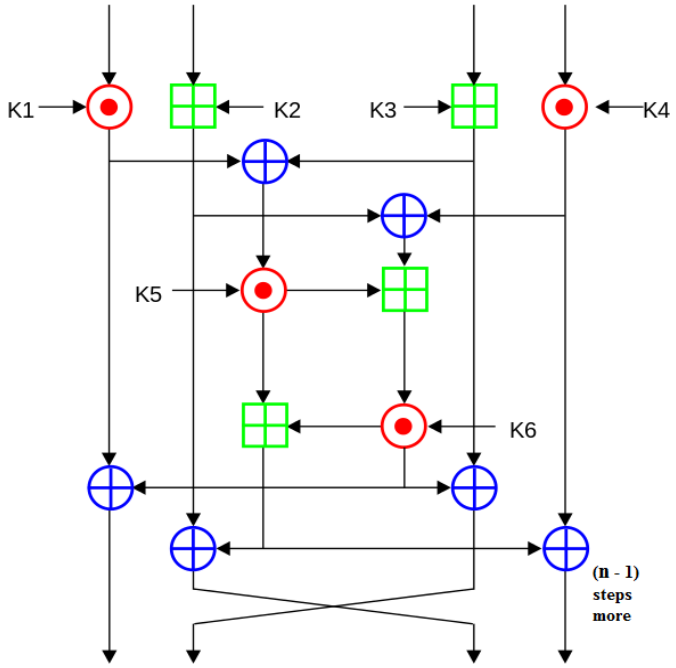

Figure – 1.4 Principle of IDEA

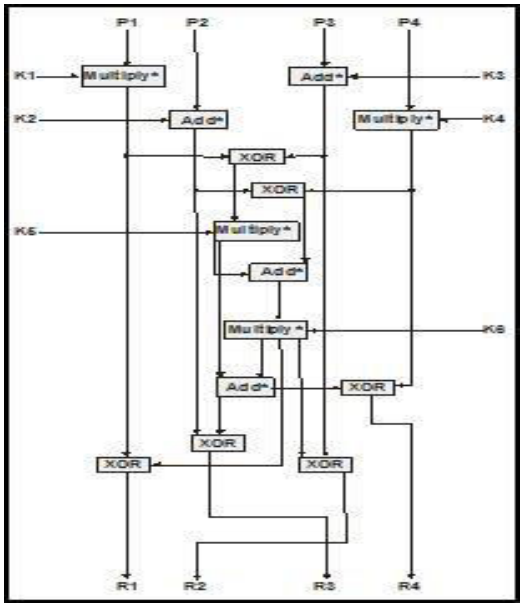

Figure – 1.5 Rounds in IDEA

Advance Encryption Standard (AES) - AES works on a plain text of size 128 bit and uses key of either of 128, 192 or 256 bits of length. It mainly performs substitution and permutation operations to get the desired cipher text [4] [8] [10].

RSA – This algorithm is used widely and very difficult to crack. This is based on block cipher technique [4] [11].

Size of block to be processed must be less than or equal to $\mathbf{log_2(n) + 1}$

Encryption and decryption will follows as:

C = Me mod n
M = Cd mod n
= (Me)d mod n
= Med mod n

The sender knows the value of C and only receiver knows the value of e.

Elliptic curve - Elliptic curve is another cryptographic technique which in comparison to RSA uses key of smaller length makes it faster [4] [8] [11]. The security aspect of this methodology depends on difficulty of determining K when provided with the values of KP and P.

K → Random Positive Integer

P → Public Key

Blowfish - Blowfish works with a key of variable size, and operates on a block of 64-bit plain text. Key-expansion and data-encryption are the two major parts of the algorithm. The later part operates on 16 rounds where each round having a permutation dependent on key and substitution on both data and key [4] [11].

Secure Hash Algorithm (SHA) - SHA stands for Secure Hash Algorithm is an algorithm designed by NIST. Having wide applications range like TLS, SSL, SSH, PGP, etc. The main work of SHA is to provide authentication not encryption, where the major authentication requirements are masquerade, content modification, sequence modification, timing modification, etc. 160 bit hash value produced from SHA-1 [4] [11].

Message Digest - The MD5 algorithm is used to verify data integrity. It produces a message hash of 128 bits. MD5 provides higher security for long messages processing and faster response. Two messages with same inputs will have different outputs and computationally infeasible to crack. MD5 offers more security than MD4 but not faster but it is not collision resistant [3] [4] [9] [10].

Comparative Analysis:

In the table 1 below we are showing a comparative analysis study of the various cryptographic algorithms namely AES, DES, RSA, Blowfish, Elliptic curve, SHA and MD5 based on key length, encryption/hashing time, decryption time, scalability, simulation speed.

Algorithm	Key Length	Encryption/Hashing time (8192 block of byte)	Scalability	Decryption Time (312 KB of data)	Simulation Speed
AES	56, 128, 192 bits	7.8 ms	Scalable	1.6 s	Medium
DES	138, 192, 256 bits	8 ms	Scalable	1.3 s	Fast
RSA	>1024 bits	13 ms	No Scalability	5.1 s	Slow
Blowfish	32 to 448 bits	6 ms	No Scalability	0.9 s	Medium
SHA	160 to 512 bits	4 – 5 ms	Scalable	Not required	Fast
Elliptic Curve	160 to 512 bits	7 ms	No Scalability	2.17	Slow
MD5	128 bits	3 ms	Scalable	Not required	Fast

TABLE 1: PERFORMANCE COMPARISON

Figure 1.4 shows the Encryption/Hashing time taken by different algorithms versus block of bytes they are processing.

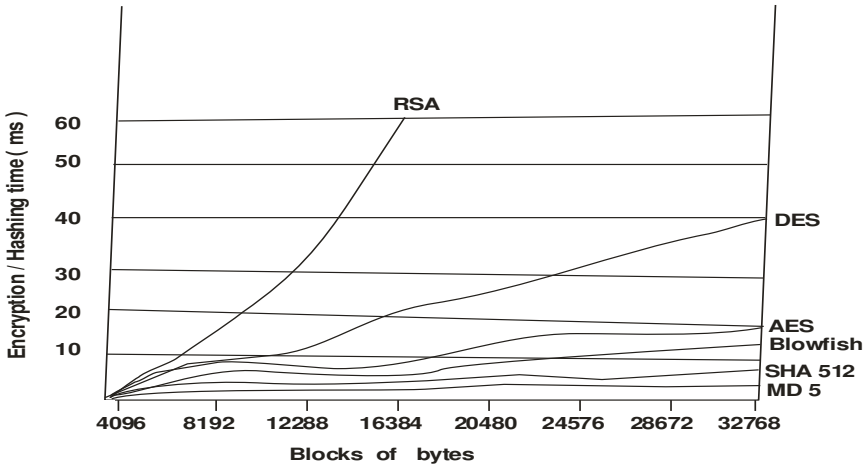

Figure 1.4 Encryption Time Vs Block of Bytes

Conclusion:

Cryptographic algorithms play a very important role in Information security. Our research work surveyed the performance of existing cryptographic methods like RSA, AES, Blowfish, DES, Elliptic Curve, MD5, SHA and RSA algorithms. Based on the experimental result it was concluded that MD5 algorithm takes least encryption time whereas, RSA takes largest encryption time.

We also found that Decryption of Blowfish algorithm is better than other algorithms, whereas, hashing based algorithms does not require decryption (as they are one way).

References:

1. Konsbruck Robert Lee, Impacts of Information Technology on Society in the new Century, 2008.
2. Stallings, W , Cryptography and Network Security: Principles and Practice, 4th ed. Englewood Cliffs, NJ: Prentice Hall.2006.

Web References:

3. http://computer.howstuffworks.com/digital-signature.htm. Retrieved 2015-04-03
4. http://www.wikinvest.com/concept/E-Commerce. (Accessed on 10 May 2015)
5. http://www.roseindia.net/services/m-commerce/mobile- commerce.shtml. (Accessed on 11 August 2015).
6. http://www.cyberciti.biz/faq/authentication-vs-authorization
7. http://searchsoftwarequality.techtarget.com/definition/cryptography
8. http://tutor2u.net/business/ict/intro_security_introduction.html. Retrieved 2015-04-03
9. http://www.legalserviceindia.com/articles/info_law.htm. Retrieved 2015-04-03
10. http://math.scu.edu/~eschaefe/book.pdf
11. http://www.netsec.org.sa/cryptography.htm